AMENDMENT TO THE SPECIFICATION

Please replace the paragraph at page 1, line 17, with the following rewritten paragraph:

In recent years, as digitization of image data evolves, there is a need for protection of a copyright of an image represented as digital data, since an image quality of the digital data is not degraded if duplicated. In addition, protection of the copyright of the image is closely related to control of accounting on the usage of the image data, and a conditional access method which is put into practical use in digital satellite broadcast is considered as a measure ~~measures~~ taken to protect the copyright of the image data.

Please replace the paragraph at page 5, line 24, with the following rewritten paragraph:

The data packets 100a(1), 100a(2), 100a(3), ..., 100a(6), 100a(7), and 100a(8) are 1st to 8th data packets included in the scrambled bit stream SB. The multiplexed bit stream MB includes data packets including compressed video data and compressed audio data corresponding to various types of program data. Therefore, the multiplexed data Sg shown in figure 10(a) includes the data packets included in the scrambled bit stream, the ECM packets, and the EMM packets for various program data.

Please replace the paragraph at page 6, line 20, with the following rewritten paragraph:

The ECM packet 110a(t), which is shown in figure 10(c), is composed of a header 110 and a key storage unit 111 which contains the encrypted scramble key Ks(t)m. The EMM packet 120a, which is shown in figure 10(d), is composed of a header 120 and a key storage unit 121 which contains the encrypted work key KWm. The scramble key Ks(t) is updated with elapse of time (t). Encrypted scramble keys Ks(1)m and Ks(2)m are obtained by encrypting a scramble key Ks(1) and a scramble key Ks(2) updated at time t=t1 and t=t2, respectively, by using the work key KW.

Please replace the paragraph at page 7, line 4, with the following rewritten paragraph:

By the way, in the above data transmission/receiving system 1000, accounting on each program data is controlled. Specifically, for a charged program which requires a contract,

corresponding program data is scrambled so that only a specified (intended) viewer which made the contract utilizes this program. Thereby, copyright of specified program data is protected. Therefore, it is difficult for viewers that ~~which~~ have not made the contract to normally reproduce and watch the content of such charged program.

Please replace the paragraph at page 7, line 13, with the following rewritten paragraph:

More specifically, the Pay Load 102 of the data packet corresponding to the charged program which is included in the scrambled bit stream SB, is scrambled, and thereby general (unintended) viewers who have not made the contract, cannot watch the charged program. To the header 100 of each data packet 100a(i), a scramble identifier Fs(i) ~~F(i)~~ indicating whether or not corresponding Pay load 102 is scrambled is affixed.

Please replace the paragraph at page 11, line 15, with the following rewritten paragraph:

In the coding scheme according to MPEG4 (MPEG4), the image signal corresponding to the scene is coded for each of the objects composing the scene, and in a decoding scheme according to MPEG4, coded data of respective objects is decoded for each object. Therefore, it is necessary to manage a copyright for each of the objects composing the scene instead of managing it for the whole scene. This is because some of the objects composing the scene do not require protection of their copyrights, and may be copied. So, MPEG4 requires object-based copyright management.

Please replace the paragraph at page 17, line 25, with the following rewritten paragraph:

According to an 8th aspect of the present invention, there is provided a data processing method for storing or transmitting a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality objects compose the scene, and the method comprises: a compression step for compressing object data corresponding to each of the plurality of

objects which compose the scene, and outputting compressed object data; an encryption step for sequentially encrypting at least compressed object data corresponding to specified objects which are predetermined among the plurality of objects according to first control information for encryption; and a data output step for outputting respective compressed object data and the scene description data to the storage medium or the transmission medium, and the encryption step includes encrypting the first control information according to second control information for encryption, dividing encrypted first control information into a plurality of information parts respectively corresponding to the specified objects, and adding the plurality of information parts to the object data of the specified objects, respectively. Therefore, the scramble key Ksb cannot be reproduced without extracting data packets of all the objects to-be-protected. That is, if object data corresponds ~~corresponding~~ to an object to-be-protected from the encrypted bit stream, this object data cannot be reproduced. This provides greatly robust protection against unauthorized copying of individual objects to-be-protected.

Please replace the paragraph at page 19, line 4, with the following rewritten paragraph:

According to a 9th aspect of the present invention, there is provided a data processing apparatus for storing or transmitting a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, and the apparatus comprises: a plurality of data compression means respectively provided for the plurality of objects, for compressing respective object data and outputting respective compressed object data; multiplexing means for multiplexing the scene description data and the respective compressed object data as individual streams and outputting a multiplexed bit stream; and encryption means for encrypting individual streams in the multiplexed bit stream which correspond to specified objects which are predetermined among the plurality of objects, to produce an encrypted bit stream, and the encrypted bit stream is output to the data storage medium or the data transmission medium. Therefore, the object data is selectively encrypted (scrambled) so that object data corresponding to the specified objects having copyrights to-be-protected is encrypted.

Please replace the paragraph at page 22, line 2, with the following rewritten paragraph:

A9

According to a 12th aspect of the present invention, there is provided a data storage medium which contains a data processing program for making a computer perform data processing for a plurality of object data respectively corresponding to a plurality of objects which compose a scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, and the data processing program comprises: an encryption step for encrypting at least object data corresponding to specified objects which are predetermined among the plurality of objects; and a data output step for outputting respective object data and the scene description data to a storage medium or a transmission medium. Therefore, selective encryption (scrambling) for the specified objects as the objects to-be-protected, is realized by software.

Please replace the paragraph at page 22, line 18, with the following rewritten paragraph:

A10

According to a 13th aspect of the present invention, there is provided a data storage medium for storing digital data used for reproducing a scene, and the digital data includes a plurality of object data respectively corresponding to a plurality of objects which compose the scene and including object data as video data or audio data, and scene description data which describes how the plurality of objects compose the scene, and is obtained by encrypting at least object data corresponding to specified objects which is predetermined among the plurality of object data and the scene description data. Therefore, at the data reading end, the encrypted (scrambled) object data or the encrypted scene description data is selectively decrypted (descrambled), whereby the encrypted data is reproduced efficiently.

Please replace the paragraph at page 26, line 5, with the following rewritten paragraph:

A11

According to an ~~a~~ 18th aspect of the present invention, in the data processing method of the 15th aspect, when deciding that the compressed and encrypted object data is reproducible, the scene description data has been read from the storage medium or received through the transmission

medium and all object data including the compressed and encrypted object data corresponding to the specified objects can be read from the storage medium or can be received through the transmission medium. Therefore, when the object data corresponding to the objects to-be-protected is all present in the storage medium or at the transmission end, and the scene description data has been read or received, object data corresponding to the specified objects is reproduced. This effectively prevents illegal usage such as unauthorized copying of the objects to-be-protected.

Please replace the paragraph at page 34, line 17, with the following rewritten paragraph:

Figure 12 is a diagram showing a structure of ~~flow of descrambling performed by~~ a data processing apparatus according to modification 2 of the third embodiment.

Please replace the paragraph at page 34, line 20, with the following rewritten paragraph:

Figure 13 is a diagram showing flow ~~a structure~~ of descrambling performed by the a data processing apparatus according to modification 1 of the third embodiment.

Please replace the paragraph at page 35, line 5, with the following rewritten paragraph:

Turning now to figure 1, there is shown a data processing apparatus 1001 of the first embodiment corresponding to a data transmission-side apparatus, which is adapted to perform coding, scrambling (encryption), and multiplexing of an image signal Dg by a coding scheme according to MPEG4, and output the resulting data to-be-transmitted Sg. An image signal input to the data processing apparatus 1001 corresponds to moving pictures of various types of programs, and an image signal for each program is coded by time sharing. The data processing apparatus 1001 is also adapted to perform coding (compression) of the image signal Dg corresponding to each frame (one scene) for each of the objects composing each scene.

Please replace the paragraph at page 36, line 18, with the following rewritten paragraph:

A15

The data processing apparatus 1001 further includes multiplexing means 17 for processing the compressed object data EDo1-EDo6 output from the respective compression means 11-16 and the scene description data Dsd according to a control signal such that these compressed data are ~~is~~ each packetized as having a fixed-bit length and then multiplexed, and outputting a multiplexed bit stream MB, and a transmission-side copyright protection device 18 for performing scrambling and packet multiplexing of the multiplexed bit stream MB, and outputting data to-be-transmitted corresponding to the output of the packet multiplexing means 80 shown in figure 9 to a transmission medium 19a or a storage medium 19b. The transmission-side copyright protection device 18 comprises scrambling means 18a for scrambling the multiplexed bit stream MB, and a CPU (central processing unit) 18b for outputting respective control signals.

Please replace the paragraph at page 41, line 20, with the following rewritten paragraph:

A16

In the scrambled bit stream SB, data parts (data regions which contain the compressed object data EDo1, EDo3, EDo4, and EDo5) of the respective data packets of the objects (1), (3), (4), and (5) having copyrights to-be-protected, have been scrambled. Also, a data region of the data packet which contains the scene description data Dsd has ~~have~~ been scrambled.

Please replace the paragraph at page 42, line 1, with the following rewritten paragraph:

A17

The data packet P'sd comprises a header Hsd and a data part Rsd which contains the scene description data Dsd following the header Hsd. The data part Rsd has been scrambled. The data packet P'(1)o1 comprises a header Ho1 and a data part Ro1 which contains the compressed object data EDo1, and the data packet P'(1)o5 comprises a header Ho5 and a data part Ro5 ~~EDo5~~ which contains the compressed object data EDo5. The data parts Ro1 and Ro5 have been scrambled. The data packet P(2)o2 of the object (2) having no copyright to-be-protected comprises a header Ho2 and a data part Ro2 which contains compressed object data EDo2 which is unscrambled. Each of the

data parts Rsd, Ro1, Ro2, and Ro5 corresponds to the Pay Load 102 of the data packet 100a(i) shown in figure 10(b), and in the data packet shown in figure 3(b), the adaptation field 101 of the data packet 100a(i) is omitted.

Please replace the paragraph at page 43, line 1, with the following rewritten paragraph:

In the conventional example, a stream to-be-scrambled (encrypted) is one compressed image data corresponding to one scene, and therefore, scrambling is controlled indiscriminately. In other words, control is performed so that all or none of the objects composing the scene are scrambled. On the other hand, in this first embodiment, since the streams to-be-scrambled (encrypted) are the plural pieces of compressed video data among the respective objects composing the scene, these compressed video data <u>are</u> ~~is~~ selectively scrambled object by object. So, commonly used video objects or audio objects, which can be copied unlimitedly, are distinguishable from objects which require protection of their copyrights, and hence, protection by scrambling corresponding compressed object data is not conducted for them.

Please replace the paragraph at page 44, line 12, with the following rewritten paragraph:

The object descriptor (1) shows that an object number and a stream type of the corresponding object 21 is "1" and MPEG4 video, respectively, and corresponding access right information is "copying unauthorized". The object descriptor (2) shows that an object number and a stream type of the corresponding object 22 is "2" and MPEG4 audio, respectively, and corresponding access right information is "copying authorized". Each of the other object descriptors (3)-(5) also shows the object number, the stream type, and the access right information, as shown in figures 4(b) <u>and 4(c)</u>. The object number is used for identifying the stream corresponding to each object (compressed object data stored in the data packet) included in the multiplexed bit stream MB.

Please replace the paragraph at page 45, line 18, with the following rewritten paragraph:

A20

The multiplexed bit stream according to MPEG4 comprises separate streams (compressed object data) for respective objects composing a scene. Therefore, scramble keys Ks(t) for as many as objects having copyrights to-be-protected (n') are generated, and the streams (compressed object data) of the objects having copyrights to-be-protected are scrambled by using corresponding scramble keys. The scramble key Ks(t) is represented by two variables, i.e., time "t" and the object number (n'). For example, a scramble key at time "t" for an "n'-th" object to-be-protected which is to be processed is represented as a scramble key Ks(n', t), although this is represented below as a scramble key Ks(n') regardless of time, for the sake of simplicity.

Please replace the paragraph at page 49, line 12, with the following rewritten paragraph:

A21

The scrambling means 18a scrambles (encrypts) the data part of the data packet which contains the compressed ~~compresses~~ object data (n) by using the scramble key Ks(n') (Step 517).

Please replace the paragraph at page 50, line 14, with the following rewritten paragraph:

A22

When it decides "No" in Step 514, the CPU 18b immediately increments the count n (Step 519), and then makes a decision on the elapsed time (Step 520).

Please replace the paragraph at page 52, line 13, with the following rewritten paragraph:

A23

While in the first embodiment the scene description according to MPEG4 has been discussed, any descriptor according to a coding scheme according to HTML, JAVA, or MPEG ~~MHEG~~ may be used so long as it represents attribute of an object.

Please replace the paragraph at page 60, line 16, with the following rewritten paragraph:

A24

The plurality of object decompression means 741-746 are provided in a way adapted to the data transmission-side apparatus 1001 and used for decompressing compressed object data EDo1-EDo6 of the first to sixth objects 21-26 (see figure 2) and outputting decompressed object data Rdo1-Rdo6. In figure 7, the object (1) decompression means 741, the object (2) decompression means 742, . . . the object (6) decompression means 746 correspond to the first, second,..., the sixth object compression ~~decompression~~ means, respectively.

Please replace the paragraph at page 62, line 10, with the following rewritten paragraph:

A25

When the multiplexed data Sg output from the data processing apparatus 1001 of the first embodiment is input to the copyright protection device 3 of the data processing apparatus 1003 of the third embodiment, the descrambling means 71 ~~descrambles~~ extracts the packetized and scrambled bit stream SB, the ECM packets, and the EMM packets from the multiplexed data Sg and descrambles the scrambled bit stream SB according to the control signal from the CPU 72.

Please replace the paragraph at page 68, line 13, with the following rewritten paragraph:

To be specific, in modification 1 of the third embodiment, the CPU 72 decides whether or not the encrypted compressed object data of all the objects to-be-protected have been decrypted (Step 820a), before the CPU 72 decides whether or not the compressed object data of all the objects have been processed by the receiving-side copyright protection device 3. When it decides "No" in Step 820a, the CPU 72 posts an instruction "limit of display" to the display means 79 (Step 820b). Thereby, the display means 79 is prohibited from reproducing the image signal corresponding to the scene including the objects to-be-protected. On the other hand, when it decides "Yes" in Step 820a, the CPU 72 makes a decision in Step 817 without Step 820b for posting the "limit of display" to the display means 79.

Please replace the paragraph at page 69, line 2, with the following rewritten paragraph:

#27

As conditions other than the conditions described above, the <u>following</u> ~~followings~~ are conceived.

Please replace the paragraph at page 70, line 18, with the following rewritten paragraph:

#28

Turning to figure 12, there is shown a data processing apparatus 1003. In the data processing apparatus 1003a, the receiving-side copyright protection device 3 of the data processing apparatus 1003 of the third embodiment has been replaced by a receiving-side copyright protection device 3a which includes descrambling means 71 for descrambling the "multiplexed and transmitted" (multiplexed) data Sg including the scrambled bit stream SB and outputting a descrambled bit stream DB_s and a CPU 72a for controlling the display means 79 according to display timing information Tsd included in the scene description data of the bit stream DB. The other components of the data processing apparatus 1003a are identical to those of the data processing apparatus of the third embodiment 1003.